Verifiable Secret Sharing as Secure Computation

(1995) (Make Corrections) (19 citations)

Rosario Gennaro, Silvio Micali
Eurocrypt'95

Bookmark in CiteULike

View or download:
mit.edu/publicatio...MITLCSTM502.pdf
Cached: PS.gz PS PDF
Image Update Help

Home/Search Bookmark Context Related

From: mit.edu/publications/pubs/pdf/
(more)
(Enter author homepages)

Links: ACM DBLP

(Enter summary)

Rate this article: 1 2 3 4 5 (best)
Comment on this article

Abstract: We present a stronger notion of verifiable secret sharing and exhibit a protocol implementing it. We show that our new notion is preferable to the old ones whenever verifiable secret sharing is used as a tool within larger protocols, rather than being a goal in itself. (Update)

Cited by: More
Verifiable Secret Redistribution - Theodore Wong Jeannette (Correct)
Unknown - (Correct)
Verifiable Secret Redistribution for - Threshold Sharing Schemes (Correct)

Similar documents (at the sentence level):
30.1%: Verifiable Secret Sharing as Secure Computation - Gennaro, Micali (1995) (Correct)
18.2%: Theory and Practice of Verifiable Secret Sharing - Gennaro (1996) (Correct)

Similar documents based on text: More All
1.5: Publicly Verifiable Secret Sharing - Stadler (1996) (Correct)
1.1: Efficient Multiparty Computations with Dishonest Minority - Damgård (1998) (Correct)
0.9: On the Complexity of Verifiable Secret Sharing and.. - Cramer.. (2000) (Correct)

Related documents from co-citation: More All
9: The Knowledge Complexity of Interactive Proof Systems (context) - Goldwasser, Micali et al. - 1985
9: Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults (context) - Chor, Goldwasser et al. - 1985
9: Secure multiparty protocols and zero-knowledge proof systems tolerating a faulty.. (context) - BEAVER - 1991

BibTeX entry: (Update)

Rosario Gennaro and Silvio Micali. Verifiable secret sharing as secure computation. In EUROCRYPT'95, volume 921 of Lecture Notes in Computer Science, pages 168--182. Springer-Verlag, 1995.
http://citeseer.ist.psu.edu/gennaro95verifiable.html More

```
@inproceedings{ gennaro95veriable,
  author = "R. Gennaro and S. Micali",
  title = "Verifiable Secret Sharing as Secure Computation",
  booktitle = "Eurocrypt'95",
  series = "{LNCS}",
  volume = "921",
  publisher = "Springer-Verlag",
  pages = "168--182",
  year = "1995",
  url = "citeseer.ist.psu.edu/gennaro95verifiable.html" }
```

Citations not processed or no citations identified.

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	4	("20020013772"|"6226618").PN.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/27 09:22
S2	2	"20050080746"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/22 10:17
S4	11	("705"/$.ccls. 713/150-194.ccls. "726"/$.ccls.) and (partial adj licen$)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/24 06:37
S5	7	("705"/$.ccls. 713/150-194.ccls. "726"/$.ccls.) and (partial adj licen$) and decrypt$	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/24 06:37
S6	239	("4200770" | "4218582" | "4272810" | "4405829" | "4424414" | "4463387" | "4528643" | "4731840" | "4757534" | "4782529" | "4803725" | "4809327" | "4825306" | "4868687" | "4868877" | "4878246" | "4879747" | "4905163" | "4926479" | "4944006" | "4995082" | "5005200" | "5130792" | "5159634" | "5191573" | "5214702" | "5220604" | "5224163" | "5224166" | "5260788" | "5261002" | "5276901" | "5315658" | "5319705" | "5347580" | "5355302" | "5369705" | "5371794" | "5412717" | "5420927" | "5497421" | "5509071" | "5519778" | "5537475" | "5557541" | "5581479" | "5588060" | "5592664" | "5604804" | "5606617" | "5636139" | "5646992" | "5646998" | "5666420" | "5673316" | "5675734" | "5706347" | "5710887" | "5745574" | "5765152" | "5796841" | "5864620" | "5889860" | "5892900" | "5915025" | "5982892" | "5991399" | "5999629").PN. OR ("6226618").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/03/25 06:38

S7	116	garay.in.	US-PGPUB;
			USPAT;
			USOCR
				OR	ON	2007/03/25 07:43

S8	11	garay.in. and ("713"/$.ccls. "726"/$.ccls. "705"/$.ccls.)	US-PGPUB;
			USPAT;
			USOCR
				OR	ON	2007/03/25 09:10

S9	27	("5485474" | "5491749" | "5491750" | "5544322" | "5604490" | "5752041" | "5758068" | "5815574" | "5832211").PN. OR ("5991414").URPN.	US-PGPUB;
			USPAT;
			USOCR
				OR	ON	2007/03/25 07:51

S10	7	S9 and license	US-PGPUB;
			USPAT;
			USOCR
				OR	ON	2007/03/25 07:51

S11	76	705/59.ccls. and threshold	US-PGPUB;
			USPAT;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2007/03/25 09:11

S12	52	705/59.ccls. and threshold and decrypt$	US-PGPUB;
			USPAT;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2007/03/25 09:12

S13	52	(threshold same license) and decrypt$	US-PGPUB;
			USPAT;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2007/03/25 09:20

S14	0	(threshold adj crypt$) and licenses	US-PGPUB;
			USPAT;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2007/03/25 09:21

S15	9	(threshold adj crypt$) and license	US-PGPUB;
			USPAT;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2007/03/25 10:16

S16	21	herzberg.in. and kutten.in.	US-PGPUB;
			USPAT;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2007/03/25 10:19

EAST Search History

S18	110	threshold adj crypto$	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/26 15:39
S19	9	(threshold adj crypto$) and license	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/26 15:39
S20	17	"705"/$.ccls. and (threshold adj crypto$)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/27 05:28
S21	21	("5005200" | "5164988" | "5224163" | "5276737" | "5422953" | "5481613"). PN. OR ("6209091").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/03/27 06:45
S22	21	licenses and vss	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/27 09:22